HISTORIA MATHEMATICA 3 (1976), 449-462

ÜBER EIN HALLENSER MANUSKRIPT DER DISSERTATION GEORG CANTORS

BY WERNER JENTSCH
MARTIN-LUTHER-UNIVERSITÄT, HALLE (SAALE) DDR

SUMMARIES

During an examination of the documents for Georg Cantor which are to be found in the libraries and archives of Halle/Saale, it turned out that a manuscript of his dissertation, written in his own hand, contains additions which go significantly beyond the version published in 1867. These additional sections are reproduced as a mathematical completion of the dissertation and as a supplement to the biography of Cantor. Some remarks of a mathematical and biographical nature are included.

Bei einer Durchsicht von Dokumenten Georg Cantors, die sich in Bibliotheken und Archiven der Stadt Halle/Saale befinden, stellte es sich heraus, dass ein von Cantors Hand geschriebenes Manuskript seiner Dissertation Zusätze enthält, die erheblich über die im Jahre 1867 veröffentlichte Dissertation hinausgehen. Zur mathematischen Abrundung der Dissertation, als Ergänzung der Biographie Cantors und zu seiner Würdigung werden die zusätzlichen Kapital hier--im wesentlichen wörtlich--wiedergegeben. Vorangestellt werden einige Bemerkungen inhaltlicher und biographischer Art.

BEMERKUNGEN

Der vorliegende Artikel soll ein kleiner Baustein zur Vervollkommnung der Biographie Georg Cantors sein. Bei einem Forscher von so grosser Bedeutung für die Nachwelt scheint es uns für eine Einschätzung der Gesamtpersönlichkeit geboten, alle Unterlagen auszuschöpfen, um auch den Beginn seiner wissenschaftlichen Arbeit möglichst genau darzustellen. Aus diesem Grunde hatte bereits Zermelo Cantors Dissertation "De aequationibus secundi gradus indeterminatis" in die *Gesammelten Abhandlungen* [Cantor 1932, 1-31] aufgenommen. Wir haben jetzt die Möglichkeit, über 100 Jahre nach Erscheinen der Dissertation eine nicht unwesentliche Ergänzung im obigen Sinne geben zu können.

In der Universität Halle, der langjährigen Wirkungsstätte Georg Cantors, wurde anlässlich seines 130. Geburtstages im März

1975 eine Ausstellung über sein Leben und Schaffen gezeigt und zu deren Vorbereitung auch ein handgeschriebenes (in deutscher Sprache abgefasstes) Manuskript seiner Dissertation "Über die Diophantischen Gleichungen zweiten Grades" durchgesehen. [1] Dabei stellte sich überraschenderweise heraus, dass dieses Manuskript ausser den (etwa aus [Cantor 1932] bekannten 11 Paragraphen noch drei weitere enthält, was bisher offenbar unbemerkt geblieben oder nicht zur Kenntnis genommen worden ist. [2]

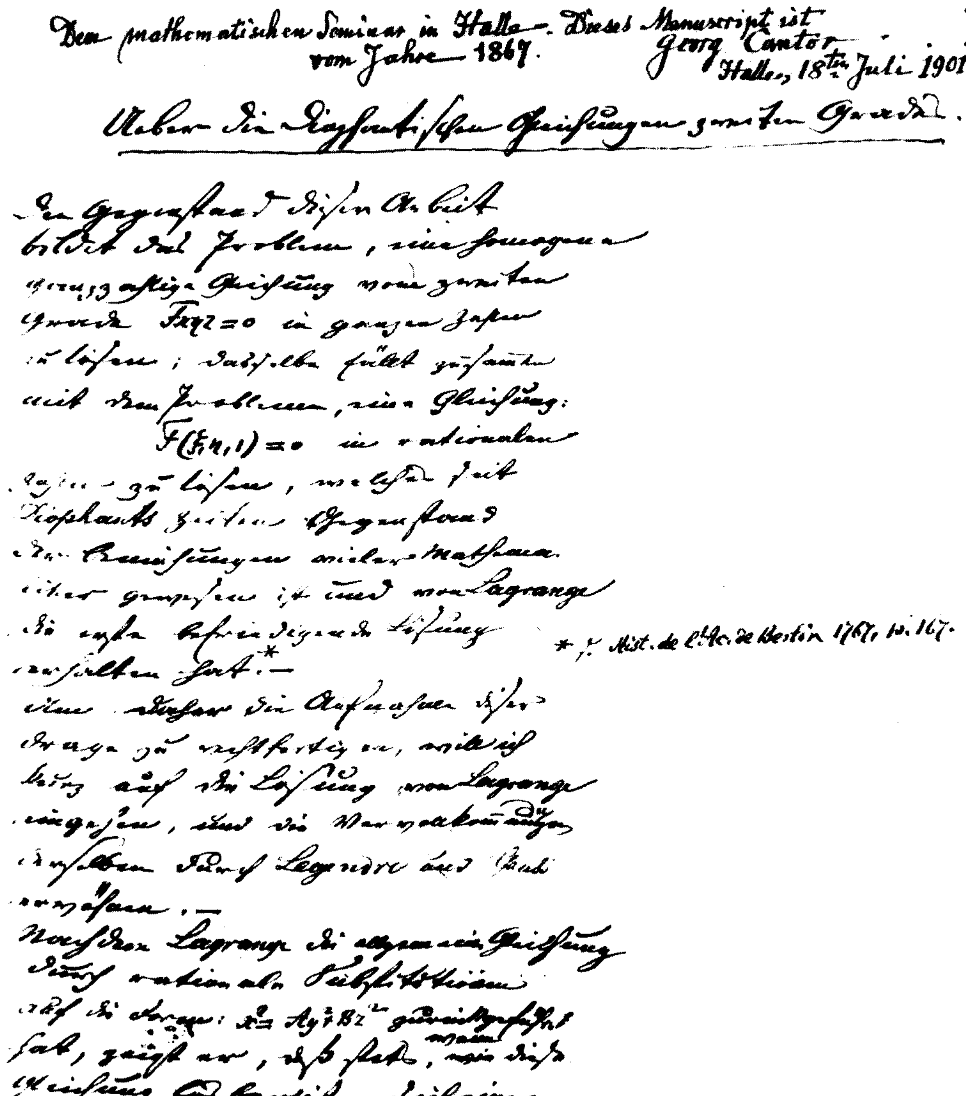
Cantors Dissertation beschäftigt sich bekanntlich mit den primitiven Lösungen der Diophantischen Gleichung $ax^2 + by^2 + cz^2 = 0$ in ganzen Zahlen. Ein Kriterium für die Lösbarkeit dieser Gleichung wurde bereits von Legendre nach Vorarbeit von Lagrange und auf anderem Wege von Gauss gewonnen. Gauss hat mit seiner Methode gleichzeitig eine Darstellung aller primitiven Lösungen in der Form $x = t^{-1}f(p,q)$, $y = t^{-1}g(p,q)$, $z = t^{-1}h(p,q)$ gegeben. Dabei sind f,g,h quadratische Formen, (p,q) durchläuft alle Paare teilerfremder Zahlen und $t = t(p,q)$ ist der grösste gemeinsame Teiler von $f(p,q)$, $g(p,q)$ und $h(p,q)$. Diese Form wird von Cantor als unbefriedigend angesehen und er baut deshalb den Gaussschen Weg weiter aus. In § 8 gelangt er zu einem Ergebnis, das eine neuartige Darstellung der Lösungsmenge ermöglicht. Später hat dies auch Dedekind in [Dirichlet 1894, 418ff.] unternommen. Sein Ergebnis ist einfacher als das Cantorsche, jedoch wird in [Bachmann 1898, 211ff.] den Gedanken und Resultaten Cantors besondere Anerkennung gezollt.

Die neu aufgefundenen Paragraphen 12 bis 14 des Cantorschen Manuskripts führen nun in summarischer Weise aus, wie das Resultat von § 8 mit der Methode von Lagrange gewonnen werden kann. Sie bilden somit eine wertvolle Ergänzung der übrigen Arbeit. Auch nach Cantors Meinung erhält das Prinzip von Lagrange "erst durch die hier [§ 12 bis § 14] vorkommende Vorstellung der Lösungssysteme seine volle Deutung."

In § 12 wird zunächst der Begriff der absoluten Gleichung eingeführt (d.i. eine solche mit quadratfreien Koeffizienten) und der Zusammenhang zwischen den primitiven Lösungen einer beliebigen Gleichung und der zugehörigen absoluten untersucht. § 13 leistet dasselbe für zwei absolute Gleichungen, die in gewisser Weise durch lineare Substitutionen auseinander hervorgehen. Schliesslich stellt § 14 die Beziehung einer beliebigen absoluten Gleichung zur pythagoreischen Gleichung $x^2 + y^2 - z^2 = 0$ her, für welche sich das angestrebte Resultat unmittelbar verifizieren lässt.

Ein Vergleich der lateinischen Ausgabe [Cantor 1867] mit dem Hallenser Manuskript zeigt, dass es sich bei jenem--von wenigen Ausnahmen abgesehen--um eine wörtliche Übersetzung der ersten 11 Paragraphen des Hallenser Manuskripts handelt. An Abweichungen seien folgende erwähnt:

1. Die beiden Schlusssätze der lateinischen Ausgabe: "Quamquam omnia quae initio commentationis polliciti sumus plane ad finem perduximus, tamen multa, quae ad explicationem methodi desiderentur



Dem mathematischen Seminar in Halle. Dieses Manuscript ist vom Jahre 1867. Georg Cantor Halle, 18ten Juli 1901

Ueber die diophantischen Gleichungen zweiten Grades.

Den Gegenstand dieser Arbeit bildet das Problem, eine homogene ganzzahlige Gleichung vom zweiten Grade $F(x,y,z)=0$ in ganzen Zahlen zu lösen; dasselbe fällt zusammen mit dem Problem, eine Gleichung: $F(\xi,\eta,1)=0$ in rationalen Zahlen zu lösen, welches seit Diophants Zeiten Gegenstand der Bemühungen vieler Mathematiker gewesen ist und von Lagrange die erste befriedigende Lösung erhalten hat.* — Um nachher die Aufnahme dieser Frage zu rechtfertigen, will ich kurz auf die Lösung von Lagrange eingehen, und die Vereinfachungen derselben durch Legendre und Gauss erwähnen. — Nachdem Lagrange die allgemeine Gleichung durch rationale Substitution auf die Form: $x^2 = Ay^2 + Bz^2$ zurückgeführt hat, zeigt er, daß stets, wenn diese Gleichung lösbar ist, sich eine

*) v. Hist. de l'Ac. de Berlin 1767, p. 167.

BILD I

omissa esse, sponte concedimus. - Hoc quidem loco annotetur veritatem theorematum in § 8 a nobis secunda demonstratione probatum esse, quae in integra inductione posita est, et methodos a nobis indagatas esse, quae via multo simpliciore ad omnes solutiones primitivas aequationum primariarum perducunt." fehlen verständlicherweise im deutschen Manuskript [Cantor 1932, 30]. Durch sie wird bereits angedeutet, dass der Verfasser ausser den veröffentlichten Ergebnissen noch weitere besass. Ein Motiv Georg Cantors (oder seines Lehrers E. E. Kummer) für das Weglassen dieser zusätzlichen Ergebnisse ist jedoch daraus nicht ablesbar. [3]

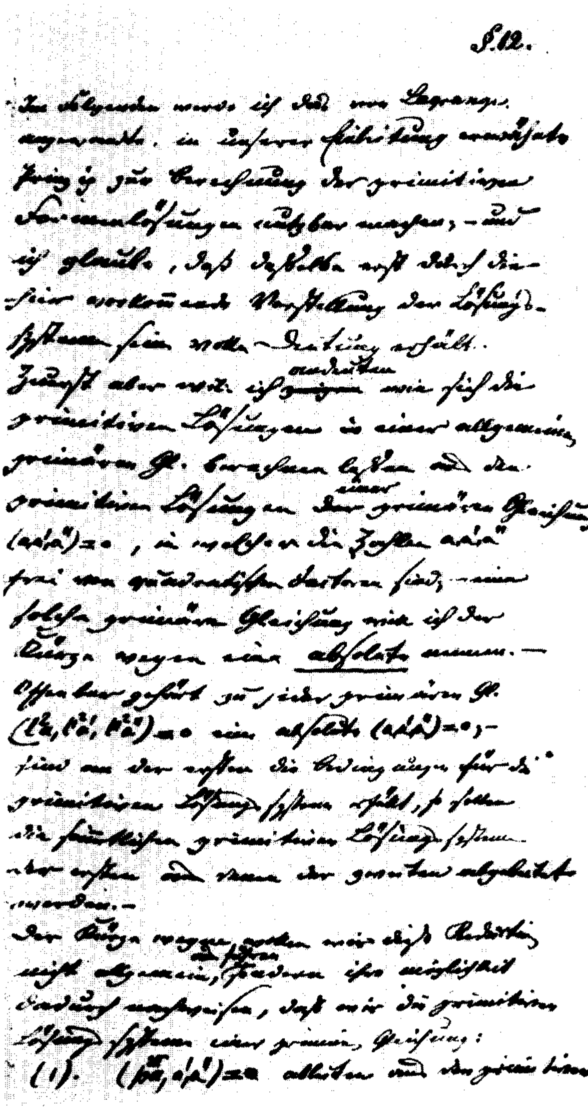


BILD II

2. Die Fussnote beim Beweis des ersten Theorems in § 8 [1932, 20], in der auf die Möglichkeit der Herleitung der angegebenen Fallunterscheidung aus vorausgesetzten Bedingungen mit Hilfe des Reziprozitätsgesetzes hingewiesen wird, erfährt im deutschen Text noch die Ergänzung: "Wollte man davon [der Herleitung] abstrahieren, so müsste man in ihnen ["den Unterscheidungen"] neue Bedingungen für die Existenz primitiver Lösungen erblicken."

3. Am Ende desselben Paragraphen wird im deutschen Text die Unterdrückung der Rechnung ausser mit ihrer Weitläufigkeit noch

damit begründet, dass spätere (nämlich die in der lateinischen Ausgabe weggelassenen) Paragraphen neben einer erneuten Verifizierung des Resultates von § 8 "eigens dazu bestimmt sind, auf leichterem Wege die Lösungssysteme zu geben." (Man vergleiche hiermit auch die oben zitierten Schlusssätze der lateinischen Ausgabe.)

Es sei noch erwähnt, dass die Originalausgabe der Cantorschen Dissertation und damit diejenige in [Cantor 1932] einige (wenn auch nicht sehr wesentliche) Fehler enthält, die im Hallenser Manuskript bemerkenswerterweise nicht vorkommen und die übrigens zum Teil in einem mir zugänglichen Exemplar von [Cantor 1867] [4] handschriftlich--wahrscheinlich von Cantor selbst--korrigiert sind.

Im folgenden werden die Paragraphen 12 bis 14 des Hallenser Manuskripts wörtlich wiedergegeben. Die Orthographie ist dem heutigen Stand angepasst; einige offensichtliche Versehen von untergeordneter Bedeutung wurden beseitigt. Die erste Seite des Manuskripts (s. Bild 1) enthält den eigenhändigen Vermerk Cantors: "Dem Mathematischen Seminar in Halle. Dieses Manuskript ist vom Jahre 1867. Georg Cantor/Halle, 18ten Juli 1901." Bild 2 zeigt die erste Seite von § 12, der das obige Zitat über die Bedeutung der §§ 12 bis 14 entnommen ist.

Wir möchten den Abdruck des nichtveröffentlichten Teils der Dissertation als eine Würdigung Georg Cantors betrachten, jedoch dürfen wir bemerken, dass ein solcher verspäteter Druck nicht völlig ungewöhnlich ist. Beispielsweise hat L. Kronecker im Jahre 1881 seine 36 Jahre vorher verfasste und damals ebenfalls nicht vollständig veröffentlichte Dissertation selbst, und zwar einschliesslich der bereits veröffentlichten Teile, im Rahmen einer Festschrift für E. E. Kummer herausgegeben.

NOTES

1. Das Manuskript befindet sich seit 1901 (s.u.) im Besitz der Bibliothek des Mathematischen Seminars bzw. der jetzigen Sektion Mathematik der Universität Halle/S.

2. Auch in der Biographie [Grattan-Guinness 1971], die etliche neue wichtige Details enthält, ist darüber nichts erwähnt. Im übrigen muss eingestanden werden, dass Stadt und Universität Halle bis vor wenigen Jahren Georg Cantor nicht die verdiente Würdigung zukommen liessen (s.aber [Kertész 1976]).

3. Möglicherweise lagen lediglich finanzielle Erwägungen zu Grunde.

4. Aus einem Sammelband *J. Thomae, G. Cantor, H. A. Schwarz, Abhandlungen* (1864-73) des Mathematischen Vereins zu Halle a.S., jetzt im Besitz der Universitäts--und Landesbibliothek Halle/ Saale.

LITERATUR

Cantor, Georg 1867 *De aequationibus secundi gradus indeterminatis* (Inauguraldissertation) Berlin

________ 1932 *Gesammelte Abhandlungen mathematischen und philosophischen Inhalts* Edited by Ernst Zermelo Berlin, Wiederabdruck Hildesheim 1962
Bachmann, P 1898 *Die Arithmetik der quadratischen Formen, Erste Abtheilung* Leipzig
Dirichlet, P G L 1894 *Vorlesungen über Zahlentheorie* Herausgegeben und mit Zusätzen versehen von R. Dedekind 4.Auflage, Braunschweich
Grattan-Guinness, I 1971 Towards a biography of Georg Cantor *Annals of Science* 27, 345-391
Kertész, A 1976 *Leben und Wirken Georg Cantors* Halle (in Vorbereitum)

DAS MANUSKRIPT

§ 12

Im Folgenden werde ich das von Lagrange angewandte, in unserer Einleitung erwähnte Prinzip zur Berechnung der primitiven Formenlösungen nutzbar machen; und ich glaube, dass dasselbe erst durch die hier vorkommende Vorstellung der Lösungssysteme seine volle Deutung erhält. Zuerst aber will ich andeuten, wie sich die primitiven Lösungen einer allgemeinen primären Gleichung berechnen lassen aus den primitiven Lösungen einer primären Gleichung $(a, a', a'') = 0$, in welcher die Zahlen a, a', a'' frei von quadratischen Faktoren sind; eine solche primäre Gleichung will ich der Kürze wegen eine *absolute* nennen. Offenbar gehört zu jeder primären Gleichung $(l^2a, l'^2a', l''^2a'') = 0$ eine absolute $(a, a', a'') = 0$; sind an der ersten die Bedingungen für die primitiven Lösungssysteme erfüllt, so sollen die sämtlichen primitiven Lösungssysteme der ersten aus denen der zweiten abgeleitet werden.

Der Kürze wegen wollen wir diese Reduktion nicht allgemein ausführen, sondern ihre Möglichkeit dadurch nachweisen, dass wir die primitiven Lösungssysteme einer primären Gleichung

(1) $$(p^{2\pi}a, a', a'') = 0,$$

ableiten aus den primitiven Formenlösungen der primären Gleichung

(2) $$(a, a', a'') = 0$$

wo wir voraussetzen, dass p eine Primzahl ist, die a entweder gar nicht oder nur in der ersten Potenz enthält. Die sukzessive Anwendung dieser Reduktion wird offenbar zu der gewünschten führen.

Es werden die sämtlichen primitiven Lösungssysteme von (2):

(3) $$\begin{array}{l} \phi_1, \psi_1, \chi_1, \\ \phi_2, \psi_2, \chi_2, \\ \dots \end{array}$$

vorausgesetzt. Jeder Zahlenlösung A, B, C von der Ordnung $O(1,1,1)$ von (1) entspricht eine Zahlenlösung von der Ordnung $O(1,1,1)$:

$$\alpha = p^{\pi}A, \quad \beta = B, \quad \gamma = C \quad \text{von (2);}$$

umgekehrt entspricht jeder Zahlenlösung $O(1,1,1)$ von (2): α,β,γ, in welcher α teilbar durch p^{π}, eine Zahlenlösung $O(1,1,1)$ A,B,C von (1). Durch diese Überlegung sieht man, dass es nur darauf ankommt, aus den Lösungen α,β,γ diejenigen auszuscheiden, bei welchen $\alpha \equiv 0 \bmod p^\pi$, und man wird so zu der Aufgabe geführt: Wenn eine primitive Form

$$\phi = \alpha xx + 2\alpha' xy + \alpha'' yy$$

mit dem Determinant $d = -\alpha'\alpha''$ gegeben ist, welcher quadratischer Rest ist von einer Primzahl p, so sollen alle Darstellungen x,y (relativ prim) gefunden werden, für welche ϕ teilbar wird durch p^π.

Diese Frage beantwortet sich leicht in Folgendem:

I. Ist p eine ungerade Primzahl, und setzt man α relativ prim gegen p voraus, so sind die sämtlichen Darstellungen enthalten in den beiden Systemen:

$$x = p^\pi\xi + h_1\eta, \qquad x = p^\pi\xi + h_2\eta,$$
$$y = \eta, \qquad\qquad y = \eta,$$

wo $\alpha h_1 + \alpha' - u_1 \equiv 0 \bmod p^\pi$, $\alpha h_2 + \alpha' - u_2 \equiv 0 \bmod p^\pi$ und u_1, u_2 die beiden Wurzeln der Kongruenz $uu \equiv d \bmod p^\pi$ sind.

II. Ist $p = 2$, so wird im Folgenden nur der Fall gebraucht, wo ϕ impropr.pr. ist; wir setzen in dieser Form $\alpha \equiv 2 \bmod 4$ voraus, und es ist $d \equiv 1 \bmod 4$; sobald $\pi \geq 2$, ist in unserer Anwendung $d \equiv 1 \bmod 8$; Die sämtlichen Darstellungen, für welche $\phi \equiv 0 \bmod 2^\pi$, sind enthalten in den 4 Systemen:

$$x = 2^\pi\xi+h_1\eta, \quad x = 2^\pi\xi+h_2\eta, \quad x = 2^\pi\xi+h_3\eta, \quad x = 2^\pi\xi+h_4\eta,$$
$$y = \eta, \quad y = \eta, \quad y = \eta, \quad y = \eta,$$

wo $\frac{\alpha}{2} h_\lambda + \frac{\alpha'-u_\lambda}{2} \equiv 0 \bmod 2^\pi$ und u_1, u_2, u_3, u_4 die vier Wurzeln von $uu \equiv d \bmod 2^{\pi+1}$ sind. Wendet man die in I., II. angegebenen Substitutionen auf eine Lösung ϕ, ψ, χ *an*, nachdem man sie zuerst den Bedingungen für ϕ entsprechend in eine äquivalente transformiert hat, so erhält man Formen

$$p^\pi \Phi, \Psi, \chi,$$

und es ist stets Φ,Ψ,χ eine Formenlösung ($H = \pm 1$) von (1). Diese Lösung ist nicht immer eine primitive. Eine genauere Untersuchung, welche wir hier unterdrücken müssen, zeigt aber, dass man auf diese Weise aus den Lösungen (3) die sämtlichen primitiven Lösungen von (1) erhalten kann. Es lässt sich eine einfache Regel angeben, nach welcher die Verbindung $ww'w''$, zu welcher $\phi\psi\chi$ gehört, zusammenhängt mit der Verbindung $WW'W''$, zu welcher die primitive Lösung $\Phi\Psi\chi$ von (1) gehört, welche aus $\phi\psi\chi$ abgeleitet werden kann.

Wir können daher den für das Folgende wichtigen Zusammenhang einer primären Gleichung mit ihrer absoluten so ausdrücken:

Jede primäre Gleichung (an welcher die Bedingungen für die primitiven Lösungen erfüllt sind)

$$(l^2 a,\ l'^2 a',\ l''^2 a'') = 0$$

hängt mit der zu ihr gehörigen absoluten Gleichung

$$(a,\ a',\ a'') = 0$$

in der Weise zusammen, dass jede primitive Lösung Ψ,Φ,χ *der* *ersteren hervorgeht aus einer zu einem bestimmten System gehörigen primitiven Lösung ϕ,ψ,χ der letzteren, indem diese durch eine Substitution*

$$x = \lambda\xi + \mu\eta \qquad y = \nu\xi + \rho\eta$$

von der Determinante $\lambda\rho - \mu\nu = \pm\, 1 1' 1''$

übergeht in

$$1\Phi \;,\; 1'\Psi \;,\; 1''\chi .$$

Es sind ferner die folgenden Bemerkungen von Wichtigkeit: Wir haben gesehen, dass stets, wenn der Determinant einer primären Form, an welcher die Bedingungen der Existenz primitiver Lösungen erfüllt sind, nicht $\equiv 0 \bmod 4$, im ganzen vier primitive Lösungssysteme

$$\phi,\ \psi,\ \chi, \qquad -\phi,\ -\psi,\ -\chi,$$
$$\psi',\psi',\chi', \qquad -\phi',-\psi',-\chi',$$

zu einer Verbindung $w,\ w',\ w''$ gehören. Diese zwei Paare unterscheiden sich durch folgende Kriterien:

1) Wenn D ungerade, $a \equiv -a' \equiv -a'' \bmod 4$ ist, so sind von den Formen ψ,χ die eine pr.pr., die andere impr.pr.; dasselbe gilt von den Formen ψ',χ'; ist aber ψ pr.pr., so ist ψ' impr.pr. und umgekehrt. Ist ψ impr.pr., so bestehen die Kongruenzen $w'\chi \equiv a\phi$, $w'\phi \equiv -a''\chi$ nicht nur mod a, sondern auch mod $2a$.

2) Wenn $D \equiv 2 \bmod 4$ und zwar $a \equiv 2 \bmod 4$, so sind ψ,χ,ψ',χ', pr. pr. Die beiden Lösungen ϕ,ψ,χ, ϕ',ψ',χ' unterscheiden sich dadurch voneinander, dass von den Quotienten $\frac{\psi}{\chi}$, $\frac{\psi'}{\chi'}$ der eine $\equiv 1 \bmod 4$, der andere $\equiv 3 \bmod 4$ *ist*.

3) Wenn $D \equiv 0 \bmod 4$ und zwar beispielsweise $a \equiv 0 \bmod 4$ und wenn ϕ impr.pr., so bestehen die Kongruenzen $w_0\psi \equiv a''\chi$, $w_0\chi \equiv -a'\psi$ nicht nur mod a, sondern auch mod $2a$, wenn w_0 die in Theorem I des § 8 definierte Zahl ist.

§ 13

Sei $(a, a', a'') = 0$ eine absolute Gleichung, an welcher

(1) $\qquad -a'a''Ra, \quad -a''aRa', \quad -aa'Ra''.$

Sei $-d = a'a'' = mn$ eine beliebige Trennung der Zahl $-d$ in zwei Faktoren, so trennen wir auch m,n durch die Identitäten $m = m'm''$, $n = n'n''$, so dass m', n' Faktoren von a' und m'', n'' Faktoren von a'' sind. Wegen (1) gibt es Zahlen t,u, welche relativ prim untereinander, so dass $ttn + uum$ teilbar ist durch a. Wir schreiben die sich daraus ergebende Gleichung in folgender Form:

(2) $\qquad ttn'n'' + uum'm'' = \mu'\nu'\mu''\nu''a_0a,$

wo μ' der gemeinsame Faktor von t und m', μ'' der von t und m'', ν' der von u und n' und ν'' der gemeinsame Faktor von u und n'' ist. Wegen der Voraussetzungen über t,u und (a,a',a'') ist a_0 rel.prim gegen d, und es sind μ',ν',μ'',ν'' paarweise rel.prim. Ist w eine beliebige Wurzel der Kongruenz $w^2 \equiv d \bmod a$, so können ausserdem

t,u so bestimmt werden, dass

$$w \equiv \frac{tn}{u} \equiv -\frac{um}{t} \ mod\ a. \tag{3}$$

Seien ausserdem w', w'' beliebige Wurzeln der Kongruenzen

$$w'^2 \equiv d' \ mod\ a', \quad w''^2 \equiv d'' \ mod\ a'',$$

und sei ϕ,ψ,χ eine zu der Verbindung w,w',w'' gehörige primitive Lösung der absoluten Gleichung $(a,a',a'')=0$, dann hat man gemäss den Definitionen (§ 6)

$$\begin{aligned} \psi tn' - \chi um'' &\equiv 0 \ mod\ a, \\ \psi um' - \chi tn'' &\equiv 0 \ mod\ a. \end{aligned} \tag{4}$$

Bevor wir diese Kongruenzen als Gleichungen schreiben, haben wir die folgenden Bemerkungen und Bestimmungen zu machen:
1) Wenn a,a',a'' ungerade sind und ϕ impr.pr., also $d \equiv 1 \ mod\ 4$ ist, wenn ferner t,u beide ungerade sind, so ist a_0 durch 4 teilbar, und die Kongruenzen (4) haben auch ihre Gültigkeit mod $2a$.
2) Ist $a \equiv 2 \ mod\ 4$ und $-a'a'' \equiv 1 \ mod\ 8$, so ist ϕ impr.pr., und auch hier wird a_0 durch 4 teilbar. Wir bestimmen die Lösung ϕ,ψ,χ den Bemerkungen am Schluss des Paragraphen [Lücke im Manuskript; evtl. ist § 14 gemeint.] zufolge dadurch näher, dass die Kongruenzen (4) ebenfalls ihre Gültigkeit mod $2a$ haben sollen.

Wir verstehen unter k die Zahl 2 in den Fällen 1) und 2), sonst aber sei $k = 1$ und setzen $a_0 = k^2 b$. Dann hat man wegen (4) mit Rücksicht auf die oben gemachten Bemerkungen

$$\begin{aligned} \psi tn' - um''\chi &= k\mu''\nu' a\psi_1, \\ \psi um' - tn''\chi &= -k\mu'\nu'' a\chi_1, \end{aligned} \tag{5}$$

in welchen Gleichungen unter ψ_1,χ_1 ganzzahlige quadratische Formen mit denselben Variablen wie in ψ,χ zu denken sind, von denen sich sogleich herausstellen wird, dass sie die Formen

$$\begin{aligned} \psi_1 &= \beta_1 xx + 2\beta_1' xy + \beta_1'' yy, \\ \chi_1 &= \gamma_1 xx + 2\gamma_1' xy + \gamma_1'' yy \end{aligned} \tag{6}$$

haben. Die Zahl $\mu''\nu'$ ist nämlich grösster gemeinsamer Faktor von tn' und um'', ausserdem relativ prim gegen ka, folglich gilt die erste Kongruenz (4) mod $k\mu''\nu' a$ und es ist ψ_1 eine ganzzahlige Form. Ebenso zeigt man, dass χ_1 eine ganzzahlige Form ist. Setzt man nun

$$\frac{m'\nu'}{\mu'} = p', \quad \frac{n'\mu'}{\nu'} = q', \quad \frac{m''\nu''}{\mu''} = p'', \quad \frac{n''\mu''}{\nu''} = q'' \quad \text{und} \tag{7}$$

$$b' = p'q'', \quad b'' = p''q', \tag{8}$$

so bestätigt man leicht die Gleichung

$$b(a\phi^2 + a'\psi^2 + a''\chi^2) = a(b\phi_1^2 + b'\psi_1^2 + b''\chi_1^2), \tag{9}$$

wenn $\phi_1 = \phi$. Nach §1 hat man aber, wenn statt xx, xy, yy, ξ,η,ζ

gesetzt wird: $a\phi^2 + a'\psi^2 + a''\chi^2 = 4aa'a''(\eta\eta-\xi\zeta)$, also hat man auch $b\phi_1^2 + b'\psi_1^2 + b''\chi_1^2 = 4bb'b''(\eta\eta-\xi\zeta)$.

Daraus geht hervor, dass ϕ_1,ψ_1,χ_1 eine Formenlösung (H = ±1) der Gleichung $(b, b', b'') = 0$ ist (s.die Endbemerkung § 1).

Die letzte Gleichung ist eine primäre, in welcher b', b'' keine quadratischen Faktoren haben, weil

$$-b'b'' = -a'a'' = d \tag{10}$$

ist. Dieselbe ist im allgemeinen keine absolute, weil in b quadratische Faktoren vorkommen können. Um das reziproke Verhalten der Gleichungen $(a,a',a'') = 0$, $(b,b',b'') = 0$ in Hinsicht auf ihre Formenlösungen $\phi\psi\chi$, $\phi_1\psi_1\chi_1$ hervortreten zu lassen, merken wir uns zu den Gleichungen (5) die Gleichungen

$$\begin{aligned} \psi_1 t\frac{n''\nu'}{\nu''} - \chi_1 u\frac{m''\mu'}{\mu''} &= k\mu'\nu'b\psi, \\ \psi_1 u\frac{m'\mu''}{\mu'} + \chi_1 t\frac{n'\nu''}{\nu'} &= -k\mu''\nu''b\chi \end{aligned} \tag{11}$$

und zu den Gleichungen (8) diese:

$$a' = p'q', \quad a'' = p''q''. \tag{12}$$

Was aber die Beziehung der beiden Formen (a,a',a'') und (b,b',b'') besonders wichtig und merkwürdig macht, liegt in dem folgenden

Theorem: Die Formenlösung ϕ_1,ψ_1,χ_1, welche in den Gleichungen (5) definiert ist und der primären Gleichung $(b,b',b'') = 0$ angehört, ist eine primitive Lösung und gehört zu der Verbindung W,W',W'' mod b, mod b', mod b'', wo diese drei Kongruenzzahlen auf folgende Weise zu bestimmen sind:

$$\begin{aligned} W &\equiv \frac{tn}{u} \equiv -\frac{um}{t} \mod b, \\ W' &\equiv -\frac{m''ua'}{\mu''\nu'}\frac{1}{kw''} \equiv \frac{m''u}{a\mu''\nu'}\frac{w''}{k} \mod q'' \\ &\equiv \frac{n'ta''}{\mu''\nu'}\frac{1}{kw'} \equiv -\frac{n't}{a\mu''\nu'}\frac{w'}{k} \mod p' \end{aligned} \Bigg\} \mod b' = p'q'',$$

$$\begin{aligned} W'' &\equiv -\frac{m'ua''}{\mu'\nu''}\frac{1}{kw'} \equiv \frac{m'u}{\mu'\nu''a}\frac{w'}{k} \mod q' \\ &\equiv -\frac{n''ta'}{\mu'\nu''}\frac{1}{kw''} \equiv \frac{n''t}{\mu'\nu''a}\frac{w''}{k} \mod p'' \end{aligned} \Bigg\} \mod b'' = p''q'. \tag{13}$$

Beweis: Die Bestätigung des zweiten Teiles wird sich jedem ergeben, wenn er darauf acht hat, dass die Lösung ϕ,ψ,χ zu der Verbindung w,w',w'' gehört und wenn er die linearen Beziehungen derselben mit ϕ_1,ψ_1,χ_1 genau anwendet.

Wir haben also nur den ersten Teil zu beweisen, dass ϕ_1,ψ_1,χ_1 eine primitive Lösung ist. Die Gleichungen (5) sind identisch in bezug auf x,y, man hat also die folgenden:

$$tn'\beta - um''\gamma = k\mu''\nu' a\beta_1, \qquad um'\beta + tn''\gamma = -k\mu'\nu'' a\gamma_1,$$
$$tn'\beta' - um''\gamma' = k\mu''\nu' a\beta_1', \qquad um'\beta' + tn''\gamma' = -k\mu'\nu'' a\gamma_1',$$
$$tn'\beta'' - um''\gamma'' = k\mu''\nu' a\beta_1'', \qquad um'\beta'' + tn''\gamma'' = -k\mu'\nu'' a\gamma_1''.$$

Man löse diese paarweise nach tn', um'' und nach tn'', um' auf mit Berücksichtigung der Gleichungen [An dieser Stelle ist im Manuskript eine Lücke gelassen; gemeint sind offenbar Gleichungen (3) aus § 5 und analoge.], dann erhält man

$$\frac{tn'}{\mu''\nu'}\alpha = k(\beta_1\gamma'-\gamma\beta_1'), \quad \frac{tn'}{\mu''\nu'}2\alpha' = k(\beta_1\gamma''-\gamma\beta_1''), \quad \frac{tn'}{\mu''\nu'}\alpha'' = k(\beta_1'\gamma''-\gamma'\beta_1''),$$
$$\frac{um''}{\mu''\nu'}\alpha = k(\beta_1\beta'-\beta\beta_1'), \quad \frac{um''}{\mu''\nu'}2\alpha' = k(\beta_1\beta''-\beta\beta_1''), \quad \frac{um''}{\mu''\nu'}\alpha'' = k(\beta_1'\beta''-\beta'\beta_1''),$$
$$\frac{tn''}{\mu'\nu''}\alpha = k(\gamma_1\beta'-\beta\gamma_1'), \quad \frac{tn''}{\mu'\nu''}2\alpha' = k(\gamma_1\beta''-\beta\gamma_1''), \quad \frac{tn''}{\mu'\nu''}\alpha'' = k(\gamma_1'\beta''-\beta'\gamma_1''),$$
$$\frac{um'}{\mu'\nu''}\alpha = k(\gamma\gamma_1'-\gamma_1\gamma'), \quad \frac{um'}{\mu'\nu''}2\alpha' = k(\gamma\gamma_1''-\gamma_1\gamma''), \quad \frac{um'}{\mu'\nu''}\alpha'' = k(\gamma'\gamma_1''-\gamma_1'\gamma'').$$

$\phi = \phi_1$ ist der Voraussetzung gemäss eine primitive Form; wir haben dasselbe von den Formen ψ_1, χ_1 zu zeigen. Die Zahlen $\frac{tn'}{\mu''\nu'}$, $\frac{um''}{\mu''\nu'}$ sind relativ prim, ebenso die Zahlen $\frac{tn''}{\mu'\nu''}$, $\frac{um'}{\mu'\nu''}$.

Bezeichnet man also mit D den grössten gemeinsamen Faktor von α, $2\alpha'$, α'', wo $D = 1$ oder $= 2$, so haben die 6 Zahlen

$$\frac{tn'}{\mu''\nu'}\alpha, \quad \frac{tn'}{\mu''\nu'}2\alpha', \quad \frac{tn'}{\mu''\nu'}\alpha'', \quad \frac{um''}{\mu''\nu'}\alpha, \quad \frac{um''}{\mu''\nu'}2\alpha', \quad \frac{um''}{\mu''\nu'}\alpha''$$

den grössten gemeinsamen Faktor D; es gibt also 6 Zahlen A,B,C,E,F,G, so dass

$$k\left\{(\beta_1\gamma'-\gamma\beta_1')A + (\beta_1\gamma''-\gamma\beta_1'')B + (\beta_1'\gamma''-\gamma'\beta_1'')C + (\beta_1\beta'-\beta\beta_1')E + (\beta_1\beta''-\beta\beta_1'')F + (\beta_1'\beta''-\beta'\beta_1'')G\right\} = D.$$

In den Fällen, wo $D = 1$, ist auch $k = 1$; man sieht aus dieser Gleichung, dass $\beta_1, \beta_1', \beta_1''$ ohne gemeinsamen Faktor sind. Sei ferner $D = 2$, $k = 1$; dieser Fall kann, wie man sich aus der Definition von k überzeugt, nur eintreten, wenn b, b', b'' ungerade werden; es kann also der gemeinsame Faktor von $\beta_1, \beta_1', \beta_1''$ nicht $= 2$ sein; ein anderer ist aber wegen jener Gleichung nicht möglich; also auch hier ψ_1 primitiv. Ist endlich $D = 2$, $k = 2$, so sieht man aus jener Gleichung unmittelbar, dass ψ_1 primitiv ist. Ganz ebenso wird gezeigt, dass χ_1 stets primitiv wird.

Es ist daher

$$\phi_1, \psi_1, \chi_1$$

eine primitive Lösung der Gleichung $(b, b', b'') = 0$.

In dem vorhergehenden gingen wir von der Gleichung $(a, a', a'') = 0$ mit einer fixierten Lösung ϕ, ψ, χ aus und kamen zu einer fixierten Lösung ϕ_1, ψ_1, χ_1 der Gleichung $(b, b', b'') = 0$. Würden wir aber die letztere Lösung gedanklich voraussetzen, so kämen wir durch die Gleichungen (11) zu der ersten, und die Wurzelverbindung w, w', w'' würde durch die Kongruenzen (13) sich aus der bekannt vorausgesetzten Verbindung W, W', W'' bestimmen lassen; denn man hat $a' = p'q'$, $a'' = p''q''$, $w \equiv \frac{tn}{u} \equiv -\frac{um}{t} \bmod a$.
Der Zusammenhang beiden Gleichungen

$$(a, a', a'') = 0, \quad (b, b', b'') = 0$$

ist also folgender:
Eine gewisse, zu der Verbindung $w \equiv \frac{tn}{u} \bmod a$, w', w'' (wo w', w'' beliebige Wurzeln der entsprechenden Kongruenzen sind) gehörige primitive Lösung ϕ, ψ, χ der ersteren hängt durch die Gleichungen (5), (11) mit einer gewissen, zu der Verbindung $W \equiv \frac{tn}{u} \bmod b$, W', W'' gehörigen primitiven Lösung ϕ_1, ψ_1, χ_1 der letzteren zusammen. Die Existenz irgendeiner von den Lösungen ϕ, ψ, χ, ϕ_1, ψ_1, χ_1 setzt die andere. Andererseits wissen wir, dass die primäre Gleichung $(b, b', b'') = 0$ in bezug auf alle ihre primitiven Lösungen in Zusammenhang steht mit der zu ihr gehörigen absoluten Gleichung, welche wir mit

$$('a, 'a', 'a'') = 0$$

bezeichnen wollen.

Dadurch tritt die absolute Gleichung $(a, a', a'') = 0$ in bezug auf eine durch die Verbindung w, w', w'' voraus fixierte Lösung ϕ, ψ, χ in Zusammenhang mit der absoluten Gleichung $('a, 'a', 'a'') = 0$ in bezug auf eine Lösung ϕ', ψ', χ' der letzteren, deren Wurzelverbindung $'w, 'w', 'w''$ a priori, d.h. ohne die Lösungen selbst nötig zu haben, aus w, w', w'' bestimmt werden kann.

Setzt man durch dieselben Operationen die absolute Gleichung $('a, 'a', 'a'') = 0$ in bezug auf die durch $'w, 'w', 'w''$ fixierte Lösung ϕ', ψ', χ' in Zusammenhang mit einer anderen $(''a, ''a', ''a'') = 0$ und diese wieder mit einer vierten $('''a, '''a', '''a'') = 0$ u.s.f., so erhält man den Begriff eines allgemeinen Zusammenhanges der absoluten auflösbaren Gleichungen in bezug auf ihre primitiven Lösungssysteme.

Wenn man daher jede absolute Gleichung, an welcher die Bedingungen der Auflösbarkeit erfüllt sind, in Zusammenhang bringen kann mit der pythagoreischen Gleichung $X^2 + Y^2 - Z^2 = 0$, an welcher die Richtigkeit des Theorems I, § 8 unmittelbar ersichtlich ist, so sieht man, dass einerseits ein vollständiger Zusammenhang aller auflösbaren absoluten Gleichungen in bezug auf ihre Lösungssysteme herrscht, andererseits das Theorem seine Richtigkeit hat für jede absolute Gleichung, bei welcher die Bedingungen erfüllt sind. Durch das Theorem in § 12 erhält alsdann jenes seine Gültigkeit für alle primären Gleichungen. Wir weisen diesen Zusammenhang mit der pythagoreischen Gleichung im folgenden Paragraphen nach.

§ 14

Um das Beabsichtigte zu zeigen, ist offenbar nur nötig, dass man in der Reihe der absoluten Gleichungen

$$(a,\ a',\ a'') = 0, \quad ('a,\ 'a',\ 'a'') = 0, \quad \ldots$$

durch besondere Disposition über die im vorigen Paragraphen definierten Operationen zu einer absoluten Gleichung

$$\left({}^{(\nu)}a,\ {}^{(\nu)}a',\ {}^{(\nu)}a''\right) = 0$$

gelangt, bei welcher der Determinant ${}^{(\nu)}D < D$ ist; denn durch sukzessive Anwendung dieser Operationen würde man schliesslich zu einer Gleichung kommen, bei welcher $D = 1$ ist, d.h. zu einer Gleichung $X^2 + Y^2 - Z^2 = 0$.

Zunächst richten wir es stets so ein, dass erster, zweiter und dritter Koeffizient der vorkommenden Gleichung der Grösse nach folgen, so dass der erste der grösste ist. Sei $(a,\ a',\ a'') = 0$ die gegebene absolute Gleichung, $w,\ w',\ w''$ die fixierte Verbindung der gedachten Lösung ϕ, ψ, χ. Wir haben dann drei Fälle zu unterscheiden:

1) $d = -a'a''$ ist positiv und von 1 verschieden. Man setze $n = 1,\ m = d,\ u = 1$, so dass $t \equiv w \mod a$ wird. Man bestimme t in den Grenzen $-\frac{a}{2}, \frac{a}{2}$ und hat dann $\nu' = \nu'' = 1$ und $tt - d = \mu'\mu''k^2 ba$. Da d kein Quadrat ist, so ist b stets von Null verschieden und $<a$. Der Determinant der Form $(b,\ b',\ b'')$ ist, weil $b'b'' = a'a''$, $<D$, umsomehr ist der Determinant der absoluten Gleichung $('a,\ 'a',\ 'a'') = 0 \quad 'D < D$.

2) $d = 1$; man mache über $u,\ m,\ n$ dieselben Voraussetzungen wie unter 1), setze aber $t = a-1$; dann wird ebenfalls $b < a$, $'D < D$.

3) Sei $d = -a'a''$ negativ. Man setze $n = a'',\ m = a',\ u = 1$ und nehme $t \equiv \frac{w}{a''} \mod a$ in den Grenzen $-\frac{a}{2}$ und $\frac{a}{2}$; dann wird $tta'' + a' = k^2\mu' ba$, $b' = \frac{a'a''}{\mu'}$, $b'' = \mu'$. Aus der offenbaren Ungleichheit $kbb''a < a(\frac{aa''}{4} + 1)$ folgt $bb'' < aa''$ und umsomehr also $'a\,'a'' < aa''$ d.h. $'d' < d'$, während wie immer $'d = d$ ist.

Ganz in der nämlichen Weise gehe man zur folgenden absoluten Gleichung über u.s.f. Man sieht, dass man eine Reihe von absoluten Gleichungen

$$(a,\ a',\ a'') = 0,\ ('a,\ 'a',\ 'a'') = 0,\ \ldots$$

erhält, in denen

$$d = 'd = ''d = \ldots,$$

hingegen

$$d' > 'd' > 'd'' \quad \ldots$$

gilt. Dies kann nur damit endigen, dass für ein gewisses (ν)

$$^{(\nu)}D < D$$

wird.

Der hier angegebene Gang zum Übergang auf die pythagoreische Form ist nun auch bei der Berechnung der primitiven Lösungen im Ganzen einzuhalten. Doch zeigen sich jedem leicht bei den einzelnen Fällen andere Modifikationen des in § 13 gezeigten Zusammenhangs, durch welche man auf kürzerem Wege zu der pythagoreischen Form gelangt. Die Rechnung besteht aus zwei verschiedenen Grundoperationen, nämlich sowohl aus dem Übergang der absoluten Gleichung $(a, a', a'') = 0$ zu der Gleichung $(b, b', b'') = 0$ und dann aus dem Übergang dieser zu der entsprechenden absoluten $('a, 'a', 'a'') = 0$. Der letzte Übergang besteht, wie wir in § 12 angedeutet haben, aus einer Transformation innerhalb der Formenlösungen und wird erst nach Vollendung des ganzen Schemas rückwärts ausgeführt. Wir haben uns nach dieser Methode eine Tabelle angelegt, welche für die aufsteigenden Determinanten D die auflösbaren absoluten Gleichungen mit ihren Lösungssystemen enthält.

****